IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION Plaintiff, vs. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendant.	C.A. No. 1:20-cv-12090-DPW

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S
MOTION FOR PRELIMINARY INJUNCTION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Federal Constitutional Provisions, Statutes, and Regulations

State Constitutional Provision, Statutes, and Legislation

Other Authorities

INTRODUCTION

The Alliance for Automotive Innovation ("Auto Innovators"), whose members include virtually all of America's vehicle manufacturers, seeks a preliminary injunction barring enforcement of Massachusetts SD645 (the "Data Law"), recently passed by ballot initiative and codified at Chapter 93K of the Massachusetts General Laws when the election results were certified on November 18, 2020. *See* Decl. of Charles Haake ("Haake Decl."), Ex. 1, SD645.

The Data Law is unconstitutional because it is preempted by federal law. The Data Law requires auto manufacturers to eliminate existing cybersecurity controls that protect core vehicle functions and thereby ensure the safe operation of vehicles within prescribed emissions limits. That state-law obligation conflicts with the requirements, purposes, and objectives of the federal National Traffic and Motor Vehicle Safety Act (the "Vehicle Safety Act"), 49 U.S.C. § 30101, *et seq.*, and the Clean Air Act, 42 U.S.C. § 7401, *et seq*. Furthermore, unless a preliminary injunction is issued to prevent the Data Law from taking effect, automobile manufacturers will suffer irreparable harm from being forced to abandon the secure vehicle systems they have spent years building, in accordance with federal law, to keep drivers and passengers safe. The loss of those systems will subject those vehicles to substantial safety and cybersecurity risks that create an imminent risk of harm to consumers—as the National Highway Traffic Safety Administration ("NHTSA"), the federal regulator charged with enforcing the Vehicle Safety Act, has already recognized. The balance of the equities and the public interest therefore also weigh heavily in favor of the requested relief.[1]

[1] The Complaint asserts a number of other claims challenging the constitutionality of the Data Law. *See* Compl. ¶¶ 116-170. Auto Innovators will pursue those claims on the merits.

Automobile manufacturers are required by the Vehicle Safety Act and the Clean Air Act to maintain the existing security and access controls that protect the electronic systems that control core vehicle safety and emissions functions. Both statutes prohibit an automaker from "making" or rendering "inoperative any . . . element of design installed on or in a motor vehicle . . . in compliance with an applicable motor vehicle safety standard" or emission standard. 49 U.S.C. § 30122; *accord* 42 U.S.C. § 7522(a)(3)(A). In other words, if an automaker has included a design element to comply with a safety standard or emission standard, then it is illegal for the manufacturer to make that design element inoperable. Automakers have designed their Vehicle Safety Act-compliant safety systems and their Clean Air Act-compliant emissions control systems to include access controls and other security measures ensuring that those systems operate safely and free from tampering.

The Data Law requires automakers to disable these security and access controls. One part of the law requires that access to vehicle on-board diagnostic systems be "standardized and not require the use of any authorization, directly or indirectly, by the manufacturer," unless a standardized authorization system administered by a third party is used across all vehicle makes and models. SD645 § 2. But no such system exists. The Data Law also would require automakers to create an open-access, bi-directional data "platform"—which also does not currently exist. Both requirements would open up to third-party access sensitive electronic vehicle safety systems, including those that control steering, acceleration, and braking, and systems that control exhaust emissions. If the Data Law is permitted to take effect, automakers will impermissibly be forced to choose between complying with their existing federal obligations to keep vehicles safe and emissions-controlled or violating the Data Law. Under longstanding principles of conflict preemption, the Data Law must fall in the face of these conflicting federal mandates. Indeed,

NHTSA has recognized that the broad access to electronic vehicle systems required by the Data Law creates substantial cybersecurity risks, and therefore is in "direct conflict" with federal law and regulations designed to mitigate those very risks. *See* Haake Decl., Ex. 4, NHTSA Testimony to Massachusetts Legislature ("NHTSA Ltr."), at 4.

The Data Law's consequences for consumer safety would be dramatic. As NHTSA further explained in its written testimony to the Massachusetts Legislature, the Data Law will require auto manufacturers to "redesign their vehicles in a manner that necessarily introduces cybersecurity risks, and to do so in a timeframe that makes design, proof, and implementation of any meaningful countermeasure effectively impossible." NHTSA Ltr. 5. The predictable effect, NHTSA added, would be to "compromise vehicle cybersecurity and public safety" (*id.*) by making it easier to hack into "safety-critical vehicle systems" that control such functions as "steering, acceleration, and braking," *id.* at 3.

The Data Law also would result in violations of the Clean Air Act's requirement that manufacturers ensure compliance with emission standards. That law subjects manufacturers to strict federal emissions-control requirements. Eliminating access controls protecting vehicle systems will enable vehicle owners or others to override the electronic systems that ensure emissions compliance. Purveyors of illegal aftermarket emissions-control "defeat" devices would have ready access to vehicle engine control modules and other system components to modify those systems to boost vehicle performance at the cost of excessive emissions.

Because the Data Law will take effect imminently—key provisions of it as soon as December 18—absent the requested injunctive relief, the substantial irreparable harms to Auto Innovators' members (and the public) would likewise be immediate. The Data Law would force members to violate federal law, starting immediately, which subjects them to federal enforcement.

The Data Law would leave members in the untenable position of having responsibility for the electronic vehicle systems at the heart of keeping vehicles safe and environmentally sound—but without the ability to control access to those systems. If a hacker were to breach a manufacturer's vehicle system as a result of the Data Law's requirement to create unprotected systems, *that* manufacturer—not the Commonwealth or the proponents of the law who stand to benefit from it—would get the blame and have its reputation and brand image irreparably tarnished. The public interest also weighs in favor of relief, because the forced introduction of untested "open access" vehicle systems that the Data Law requires will create unnecessary dangers on Massachusetts roads and highways. A preliminary injunction to preserve the status quo until the challenges to the Data Law can be resolved is therefore warranted.

BACKGROUND

Auto Innovators' members are the country's leading car and light truck manufacturers. Haake Decl. 1-2. These companies produce nearly 99 percent of the cars and light trucks sold in the United States. *Id.* The vehicles they manufacture are sold throughout the country, including in Massachusetts, both through dealership sales and aftermarket used sales. *See* Decl. of Heini Schulz of BMW of North America, LLC ("BMW Decl.") ¶ 3; Decl. of Mark Chernoby of FCA USA LLC ("FCA Decl.") ¶¶ 2-3; Decl. of Michael Westra of Ford Motor Co. ("Ford Decl.") ¶¶ 5-6; Decl. of Paul E. Copses of General Motors LLC ("GM Copses Decl.") ¶¶ 2-3; Decl. of John Vilkinofsky of Honda R&D America, LLC ("Honda Decl.") ¶ 3; Decl. of William John Cook of Hyundai Motor America ("Hyundai Cook Decl.") ¶ 2; Decl. of James Morgan of Jaguar Land Rover Ltd. ("JLR Decl.") ¶ 2; Decl. of Orth Hedrick of Kia Motors America, Inc. ("Kia Hedrick Decl.") ¶ 3; Decl. of Taro Ando of Mazda Motor of America ("Mazda Decl.") ¶¶ 3-4; Decl. of Kenneth Lin of Subaru of America, Inc. ("Subaru Lin Decl.") ¶ 3; Decl. of David J. Stovall of Toyota Motor Sales, U.S.A. ("Toyota Stovall Decl.") ¶ 3.

Vehicles sold in the United States today bear little resemblance to the vehicles of yesteryear. Cars today are computers on wheels. Even as of 2015, "a typical automobile feature[d] over 100 microprocessors, 50 electronic control units (ECUs), five miles of wiring and 100 million lines of [software] code." Haake Decl. Ex. 2, U.S. Dep't of Trans., NHTSA, *Report to Congress: "Electronic System Performance In Passenger Motor Vehicles"* 2 (Dec. 2015), *available* at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/electronic-systems-performance-in-motor20vehicles.pdf. These electronic systems "enable[] safer and more fuel-efficient vehicles" and provide "many safety, security, convenience, comfort, and efficiency functions for vehicle operators through interconnections and communications with other onboard electronics systems." *Id.* At the same time, these systems have "increased complexities in the design, testing, and validation of automotive systems," which in turn "raise general challenges" of ensuring the safety and security of vehicles. *Id.*

Auto Innovators' members use robust security and access control measures to ensure the safety of their vehicles and vehicle systems—and therefore drivers and passengers—as required by federal law. These controls are an integral part of critical vehicle functions governed by the Vehicle Safety Act and stringent federal motor vehicle safety standards promulgated by NHTSA under that Act. BMW Decl. ¶ 22; FCA Decl. ¶¶ 22-23, 26; Ford Decl. ¶¶ 13, 15-17; Honda Decl. ¶¶ 18-21; Declaration of John Robb of Hyundai America Technical Center, Inc. - Hyundai ("Hyundai Robb Decl.") ¶¶ 6-18; Declaration of John Robb of Hyundai America Technical, Center, Inc. – Kia (Kia Robb Decl.") ¶¶ 7-8; JLR Decl. ¶¶ 20-23; ("Mazda Decl. ¶¶ 17, 19-20, 22; Decl. of Kenichi Yamamoto of Subaru Corporation ("Subaru Yamamoto Decl.") ¶¶ 3-4, 6; Decl. of Stephen McFarland of Toyota Motor N.A., Inc. ("Toyota McFarland Decl.") ¶¶ 3-5, 7; *see also* Haake Decl. Ex. 3, NHTSA, *Cybersecurity Best Practices for Modern Vehicles* (Oct. 2016).

Manufacturers are prohibited from removing these controls by federal law. 49 U.S.C. § 30122(b) ("manufacturer . . . may not knowingly make inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard").

Auto Innovators' members also use security and access controls to protect systems regulating exhaust emissions. And pursuant to the Clean Air Act, the EPA imposes strict emissions requirements on manufacturers. *See, e.g.*, 40 C.F.R. pt. 86 (Control of Emissions from New and In-Use Highway Vehicles and Engines); 49 C.F.R. pts. 523, 531, 533, 536, & 537 (2017 and Later Model Year Light-Duty Vehicle Greenhouse Gas Emissions and Corporate Average Fuel Economy Standards). Many of these requirements impose ongoing obligations on manufacturers that continue even after the vehicles are sold. *See, e.g.*, 40 C.F.R. § 86.1845-04 (discussing required "in-use verification testing" on post-sale vehicles at regular mileage intervals).

Manufacturers' access controls help to prevent vehicle owners or others from accessing vehicle systems to tamper (illegally) with the emissions controls—which they may wish to do in order to increase vehicle performance. FCA Decl. ¶ 27; Honda Decl. ¶ 23; Toyota McFarland Decl. ¶ 6; *see* 42 U.S.C. § 7522(a)(3)(A) (prohibiting the installation of defeat devices). Manufacturers are prohibited from removing these controls by federal law. 42 U.S.C. § 7522(a)(3)(A) ("[manufacturer may not] remove or render inoperative any device or element of design installed on or in a motor vehicle or motor vehicle engine in compliance with [emissions] regulations").

Manufacturers continually refine their controls over access to electronic vehicle systems to ensure that those systems remain secure. Current measures used by members include, for instance, encryption keys, unique IDs, password protections, asymmetric keys or identity certificates

exchanged between vehicle systems and a member's servers, authorized message requirements, secure boot, secure storage, network domain segregations, and firewalls—all designed to control and protect the flow of messages in vehicle systems to prevent cybersecurity threats. BMW Decl. ¶¶ 20, 22; FCA Decl. ¶¶ 22-23, 26; Ford Decl. ¶¶ 13, 15-16; Decl. of Kevin Tierney of General Motors Co. ("GM Tierney Decl.") ¶¶ 4-5, 7; Honda Decl. ¶¶ 18-19, 21; Hyundai Robb Decl. ¶¶ 6-8; JLR Decl. ¶¶ 20-23; Mazda Decl. ¶¶ 19-20, 22; Subaru Yamamoto Decl. ¶¶ 4, 6; Toyota McFarland Decl. ¶ 3. By using these security and access controls, members can ensure that only individuals and entities authorized by the manufacturer can access (or alter) vehicle systems and data that control core vehicle functions such as steering, acceleration, and braking. FCA Decl. ¶¶ 22, 26; Ford Decl. ¶¶ 15; Honda Decl. ¶ 18; Mazda Decl. ¶¶ 12, 20, 22; Subaru Yamamoto Decl. ¶ 3; Toyota McFarland Decl. ¶ 5.

At the same time, Auto Innovators' members have designed their vehicle systems to safely provide vehicle owners (and the repair shops of their choice) with the vehicle data necessary for diagnosis, repair, or maintenance. BMW Decl. ¶ 10; FCA Decl. ¶¶ 14-15; Ford Decl. ¶¶ 7, 13; GM Copses Decl. ¶ 5; Honda Decl. ¶ 10; Decl. of Omar Rivera of Hyundai Motor America ("Hyundai Rivera Decl.") ¶ 2; Mazda Decl. ¶ 10; Subaru Lin Decl. ¶ 7; Toyota Stovall Decl. ¶ 9. That is consistent with pre-existing Massachusetts law, which already mandates that auto manufacturers "shall provide access to their onboard diagnostic and repair information system[s]" and that, to the extent any proprietary device were necessary to access the data on those systems, that device be made "available to independent repair facilities upon fair and reasonable terms." Mass. Gen. L. ch. 93K, § 2(d)(1). With years of time and effort, members have designed their vehicle systems to allow this access to necessary data, while also retaining the series of security controls to help ensure that this access does not compromise other vehicle systems and data that

could create risks for vehicle safety. FCA Decl. ¶¶ 14-17, 22-23, 26; Ford Decl. ¶¶ 7, 16; Honda Decl. ¶¶ 8, 10-11; Mazda Decl. ¶¶ 10-12, 19-22.

The Data Law upends this balance by sweeping beyond the data *necessary* for the diagnosis, repair, or maintenance of the vehicle. Instead, it reaches what it calls "[m]echanical data," defined broadly to include "*any* vehicle specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for *or otherwise related to* the diagnosis, repair or maintenance of the vehicle." SD645 § 1 (emphasis added). By referring to data "otherwise related to" diagnosis, repair, or maintenance, the Data Law, if read to its logical extreme, would extend to cover much of the data generated, stored in, or transmitted by a motor vehicle. *See* FCA Decl. ¶ 18; Honda Decl. ¶ 14; JLR Decl. ¶ 15; Mazda Decl. ¶ 15; Toyota Stovall Decl. ¶ 13.

With respect to "mechanical data" and "telematics system data," the law then imposes broad access requirements. Section 2 of the Data Law requires that access to vehicle on-board diagnostic systems be "standardized and not require any authorization by the manufacturer, directly or indirectly," unless a standardized authorization system is used across all vehicle makes and models and is administered by a third party. SD645 § 2.

Section 3 of the Data Law requires each manufacturer that "utilizes a telematics system" in any of its vehicles sold in Massachusetts to equip any vehicle sold in Massachusetts with a novel "open access" vehicle telematics platform. SD645 § 3. The Data Law defines a "telematics system" as "any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such [data] . . . utilizing wireless communications to a remote receiving point where it is stored." *Id.* § 1. Vehicles utilizing those systems would have to be equipped with "an inter-operable, standardized and open access platform across all . . . makes and models"

"[c]ommencing in model year 2022." *Id.* § 3. That platform (a) must further be "directly accessible" by the vehicle owner through an (undefined and non-existent) "mobile-based application" as well as by independent repair facilities; (b) must allow these parties "to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair;" (c) and must be "capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform"—*i.e.*, without auto manufacturers having any control over it. *Id.*[2]

Finally, Section 5 of the Data Law imposes a broad range of penalties for violators. It permits vehicle owners and independent repair shops to sue auto manufacturers for violations of the statute and recover treble damages or a minimum penalty of $10,000 per event. SD645 § 5. It also subjects manufacturers to "any remedy authorized by chapter 93A" of the Massachusetts General Laws, *id.*, meaning that if an auto manufacturer were to be unable to develop the data access systems required by the Data Law, the Commonwealth could seek injunctive relief against it, *see* Mass. Gen. L. ch. 93A, § 2(c), up to and including exclusion from the Massachusetts auto market entirely, *id.* § 8. Further, the law does not on its face limit liability to sales by new vehicle dealers in Massachusetts; instead, it applies to any "manufacturer of motor vehicles sold in the Commonwealth." SD645 § 3. Thus, the text of the Data Law would seem to impose liability on an automaker if *any party* were to sell a vehicle in Massachusetts, including a used vehicle originally sold elsewhere. Manufacturers could thus face these substantial penalties if *any party* were to sell a vehicle in Massachusetts, including a used vehicle originally sold elsewhere, that did not comply with the Data Law's onerous new requirements. *See id.* § 5.

[2] Section 4 of the Data Law directs the Attorney General "to establish for prospective vehicle owners a motor vehicle telematics system notice" that certain classes of dealerships would have to provide to prospective owners. SD645 § 4.

The Data Law imposes its novel requirements almost immediately. The standardization requirements in section 2 and the penalties in section 5 go into effect on December 18—days from now.[3] Because section 2 applies to model year 2018 and beyond, it applies to vehicles currently for sale on dealer lots, which have necessarily already been designed and produced. *E.g.*, FCA Decl. ¶ 4; Ford Decl. ¶ 6; GM Copses ¶ 4; Honda Decl. ¶ 4; Hyundai Cook Decl. ¶ 3; Mazda Decl. ¶ 4. The "open access" platform requirements in section 3 go into effect beginning with model year 2022 vehicles, SD645 § 3, which is for all practical purposes also immediate. Consistent with standard industry lead times, Auto Innovators' members have already completed the design and testing process for model year 2022 vehicles and plan to sell those vehicles in the first quarter of 2021, as soon as January 2021. Decl. of Anthony Corsetti of General Motors LLC ("GM Corsetti Decl.") ¶ 3; *see also, e.g.*, FCA Decl. ¶ 5 (March 1, 2021); JLR Decl. ¶ 4 (May 2021); Subaru Lin Decl. ¶ 3 (spring 2021).

While the ballot initiative was under consideration, in June 2020, the Massachusetts Legislature's Joint Committee on Consumer Protection and Professional Licensure asked NHTSA to provide written testimony regarding whether and to what extent the Data Law, if enacted and enforced, might pose safety and cybersecurity risks against which federal law is designed to safeguard. NHTSA expressed grave and substantial concerns about the requirements in sections 2 and 3 of the Data Law. NHTSA Ltr. 2, 4. NHTSA concluded that mandating an open access vehicle platform accessible to third parties—particularly one allowing parties to overwrite vehicle data—would conflict with federal regulatory obligations, putting the public at risk by

[3] Auto Innovators' Complaint referred to December 3, 2020 as the Data Law's operative date—30 days after the November 3, 2020 election. *See* Compl. ¶¶ 21, 164. But the election results were not certified until November 18, 2020, *see* Mass. Gen. L. ch. 54, § 112, so the Data Law's operative date is December 18, 2020, *see* Mass. Const. amends. art. 48, pt. V, § 1.

compromising the integrity of such vital vehicle functions as braking, acceleration, and steering. *Id.* at 2. The Data Law's requirements, in tandem with the timeframe for those requirements to take effect, "would require [manufacturers] to remove all access controls from their telematics systems, *including controls designed to ensure the security of safety-critical systems*." *Id.* at 3 (emphasis added). And doing so "would raise *substantial safety risks* for American families." *Id.* (emphasis added).

Following a successful ballot initiative, the Data Law was certified on November 18, 2020. Haake Decl. ¶ 3. Two days later, Auto Innovators filed suit. ECF No. 1.

ARGUMENT

Auto Innovators is entitled to a preliminary injunction because (1) it is "likely to succeed on the merits"; (2) it is "likely to suffer irreparable harm in the absence of preliminary relief"; (3) "the balance of equities tips in [its] favor"; and (4) an injunction "is in the public interest." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008). If the movant demonstrates that it will suffer irreparable harm absent the injunction and the balancing of the equities tips "decidedly in the movant's favor," then the movant must demonstrate only that there exist "sufficiently serious questions going to the merits to make them a fair ground for litigation" in order to be entitled to a preliminary injunction. *Capability Grp. Inc. v. Am. Express Travel Related Servs. Co.*, 706 F. Supp. 2d 146, 160 (D. Mass. 2010). For the reasons we explain below, the Data Law is unconstitutional, and compliance with the Data Law would create immediate risks to the safety of the driving public and impose massive, unrecoverable costs on manufacturers. Accordingly, all four preliminary injunction factors are satisfied.

I. Auto Innovators Is Likely To Succeed On The Merits.

The first factor in the preliminary injunction analysis requires the movant to show that it is "likely to succeed on the merits" of its claims. *Winter*, 555 U.S. at 20. Auto Innovators meets that

burden because the Data Law conflicts with, and therefore is preempted by, the Vehicle Safety Act, related federal vehicle safety regulations, and the Clean Air Act.

State laws must fall in the face of conflicting federal law. It is a "fundamental principle of the Constitution" that "Congress has the power to preempt state law." *Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 372 (2000) (citing U.S. Const. art. VI, cl. 2). The Supremacy Clause directs that the "laws of the United States . . . shall be the supreme law of the land; and the Judges in every state shall be bound thereby, any Thing in the Constitution or laws of any State to the contrary notwithstanding." U.S. Const. art. VI, cl. 2.

Congress may preempt state law expressly in statutory text or "implicitly," when "state law is in actual conflict with federal law." *Freightliner Corp. v. Myrick*, 514 U.S. 280, 287 (1995) (internal citations omitted). Conflict preemption exists "where it is impossible for a private party to comply with both state and federal requirements, or where state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Id.* (internal quotations omitted).

Here, the Data Law is invalid under well-established conflict-preemption principles. Its requirement that auto manufacturers abandon existing cybersecurity controls that protect core vehicle functions—and thereby ensure the safe operation of vehicles within prescribed emissions limits—runs headlong into the requirements, purposes, and objectives of the Vehicle Safety Act and the Clean Air Act.

A. The Data Law Is Preempted By The Vehicle Safety Act.

Preemption claims based on the Vehicle Safety Act are analyzed under "ordinary pre-emption principles"; the Act imposes no "special burden" on a preemption claim. *Geier v. Am. Honda Motor Co., Inc.*, 529 U.S. 861, 870 (2000). Courts routinely hold that the Vehicle Safety

Act preempts conflicting state law. *See, e.g.*, *id.* at 881 ("[When state law stands] as an obstacle to the accomplishment and execution of the important means-related federal objectives [of the Vehicle Safety Act] it is preempted."); *Wood v. Gen. Motors Corp.*, 865 F.2d 395, 408 (1st Cir. 1988) (holding that a state-law cause of action "stands as an obstacle" even where its goal "might be the same as that of the [Motor Vehicle] Safety Act . . . because it interferes with the *method* by which Congress intended to meet this goal."); *Courtney v. Mitsubishi Motors Corp.*, 926 F. Supp. 223, 226 (D. Mass. 1996) (holding that federal motor vehicle safety standards promulgated under the Act impliedly preempted state law regarding air bag safety).

Congress passed the Vehicle Safety Act over a half century ago to "reduce traffic accidents and deaths and injuries resulting from traffic accidents" through "motor vehicle safety standards" and "needed safety research and development." 49 U.S.C. § 30101. The Act delegated authority to the Secretary of Transportation, who in turn delegated it to NHTSA. 49 C.F.R. § 1.95(a). With the "broad authority granted to" it by Congress, *Verna by Verna v. U.S. Suzuki Motor Corp.*, 713 F. Supp. 823, 827 (E.D. Pa. 1989), NHTSA focuses on its core objectives—"saving lives, preventing injuries, and reducing economic costs resulting from road traffic crashes through education, research, safety standards, and other enforcement activity," *Butler v. Daimler Trucks of N.A., LLC*, 433 F. Supp. 3d 1216, 1241 (D. Kan. 2020).

The Vehicle Safety Act, among other things, specifically requires auto manufacturers not to remove or otherwise degrade their vehicles' critical safety features. *See* 49 U.S.C. § 30122. A "manufacturer . . . may not knowingly make inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard prescribed under this chapter." *Id.* § 30122(b). But the Data Law requires auto manufacturers to do just that.

Federal Law Requires Manufacturers to Maintain Cybersecurity Protections for Vehicle Systems. NHTSA's motor vehicle safety standards regulate core vehicle functions—such as braking and acceleration—as well as passenger safety features like air bags. *See, e.g.*, 49 C.F.R. § 571.121 (air brake systems); *id.* § 571.124 (accelerator control systems); *id.* C.F.R. § 571.208 (air bags). These standards reach broadly to include all components related to those functions. For example, the federal motor vehicle safety standard for accelerator control systems encompasses "all vehicle components, except the fuel metering device, that regulate engine speed in direct response to movement of the driver-operated control and that return the throttle to the idle position upon release of the actuating force." *Id.* § 571.124.

All of these vehicle functions are controlled electronically. *See, e.g.*, FCA Decl. ¶ 16; Honda Decl. ¶¶ 6, 18; Mazda Decl. ¶ 12 And as an integral part of the design of the components involved in—and the systems that control—these vehicle functions, NHTSA requires manufacturers to install and maintain rigorous access and security controls as safeguards to prevent cybersecurity threats that might compromise those functions. NHTSA, *Cybersecurity Best Practices for Modern Vehicles* (Oct. 2016).[4] Automakers recognize that they are obligated to

[4] As part of its supervisory authority to promote vehicle safety under the Vehicle Safety Act, NHTSA develops guidance like the cybersecurity best practices guide, to explain to manufacturers how to comply with federal-law obligations. *See, e.g.*, NHTSA, *Cybersecurity Best Practices for Modern Vehicles* (Oct. 2016) (discussing NHTSA's intent to encourage "proactively adopting and using available guidance such as this document and existing standards and best practices"). This guidance allows NHTSA to react nimbly to the evolution of cybersecurity threats and buttresses NHTSA's promulgation of formal safety standards, which recognize that vehicles increasingly depend on sophisticated technology to control essential functions. *See, e.g.*, 49 C.F.R. § 571.126 (mandating minimum safety standards for electronic stability control systems in lightweight passenger vehicles, which controls among other things vehicle steering, braking, and speed by computer means). Auto Innovators' members rely on this guidance to ensure that their increasingly electronic vehicle systems continue to meet rigorous federal safety standards and avoid creating safety defects that would require recalls. *See, e.g.*, FCA Decl. ¶ 26; Ford Decl. ¶ 17; GM Tierney Decl. ¶ 7; Hyundai Robb Decl. ¶ 8; JLR Decl. ¶ 23; Kia Robb Decl. ¶ 8; Mazda Decl. ¶ 22; Subaru Yamamoto Decl. ¶ 6.

satisfy NHTSA's cybersecurity requirements. *E.g.*, FCA Decl. ¶ 26; Ford Decl. ¶ 17; GM Tierney Decl. ¶ 7; Hyundai Robb Decl. ¶ 8; JLR Decl. ¶ 23; Kia Robb Decl. ¶ 8; Mazda Decl. ¶ 22; Subaru Yamamoto Decl. ¶ 6.

Indeed, NHTSA has enforced the obligation to include cybersecurity protections in vehicle systems that control core vehicle functions. In 2015, NHTSA found that some Chrysler vehicles had a flaw in their radio software security that "could allow unauthorized third-party access to some networked vehicle control systems." Haake Decl. Ex. 5, FCA, Safety Recall R40 / NHTSA 15V-461, Radio Security Vulnerability 2 (July 2015), https://static.nhtsa.gov/odi/rcl/2015/RCRIT-15V461-7681.pdf. Specifically, NHTSA determined that third-party "[e]xploitation of the software security vulnerabilities could lead to exposing the driver, the vehicle occupants or any other individual or vehicle with proximity to the affected vehicle to a potential risk of injury." *Id.* Ultimately, Chrysler worked with NHTSA to issue a voluntary recall of 1,410,000 vehicles to repair the software vulnerability.[5]

Automakers protect their vehicle systems against unauthorized access by including a variety of protections, such as encryption keys, unique IDs, password protections, asymmetric keys or identity certificates exchanged between vehicle systems and a member's servers, authorized message requirements, secure boot, secure storage, network domain segregations, and firewalls designed to control and protect the flow of messages in vehicle systems. *See* FCA Decl. ¶ 23; Ford

[5] The Vehicle Safety Act gives NHTSA broad, congressionally delegated supervisory authority over auto manufacturers to require recalls for safety-related defects. 49 U.S.C. §§ 30118-120. NHTSA can exercise that power formally by requiring manufacturers to recall vehicles that do "not comply with an applicable motor vehicle safety standard" or that have "a defect related to motor vehicle safety" 49 U.S.C. § 30118(b)(1). When NHTSA issues a notice of a safety-related defect, manufacturers often work with NHTSA to conduct a voluntary recall; though voluntary, NHTSA retains control of the process. *See, e.g.*, *Ctr. for Auto Safety v. NHTSA*, 452 F.3d 798, 802 (D.C. Cir. 2006) ("Even though voluntary recalls are initiated by a manufacturer, NHTSA retains full authority under the Act to oversee and regulate *any* recall.").

Decl. ¶¶ 13; GM Tierney Decl. ¶¶ 5, 7; Honda Decl. ¶ 19; Hyundai Robb Decl. ¶ 7; Kia Robb Decl. ¶ 7; Mazda Decl. ¶ 20; Subaru Yamamoto Decl. ¶ 6. And members continually refine the controls needed to protect their vehicle systems, in an effort to stay a step ahead of increasingly sophisticated cybersecurity threats. *E.g.*, FCA Decl. ¶ 25; GM Tierney Decl. ¶ 6; Honda Decl. ¶ 20; Hyundai Robb Decl. ¶ 8; Mazda Decl. ¶ 20.

These access and security controls ensure that members' vehicle systems are isolated from external connections, preventing access—or mitigating the effects of any access—by unauthorized third parties to core vehicle functions, including the ability to control vehicles remotely. *E.g.*, FCA Decl. ¶ 26; Ford Decl. ¶¶ 15-16; GM Tierney Decl. ¶ 7; Honda Decl. ¶ 21; Mazda Decl. ¶ 20; Subaru Yamamoto Decl. ¶ 6.

As a further design feature to protect core vehicle functions, members retain control over authorization to access or modify data that is unnecessary to vehicle diagnostics, repair, or maintenance, and the vehicle systems that house that data. This helps to ensure, for instance, that only those with members' authorization can access a vehicle's Controller Area Network (CAN) bus messages, which communicate among the various components of vehicle systems and play a key role in critical vehicle functions such as steering, acceleration, and braking. *E.g.*, FCA Decl. ¶¶ 16-17; Ford Decl. ¶ 15; Hyundai Rivera Decl. ¶¶ 4-5; Decl. of Lewis Thompson of Kia Motors, America, Inc. ("Kia Thompson Decl.") ¶¶ 5-6; Mazda Decl. ¶ 12.

The Data Law Requires Manufacturers to Violate Federal Law. By mandating an "open access" security regime over vehicle systems that generate data, the Data Law requires auto manufacturers to violate Section 30122 of the Vehicle Safety Act by "mak[ing] inoperative" the access and security safeguards that they built into the design of important vehicle components to

comply with federal safety standards. 49 U.S.C. § 30122(b). The Data Law does this in several ways.

First, the Data Law removes the ability of manufacturers to control who is authorized to access some of their vehicle systems—effective immediately. It mandates that "on-board diagnostic systems" in any vehicles "sold in the Commonwealth" be "standardized and not require any authorization by the manufacturer, directly or indirectly," unless a standardized authorization system is used across all vehicle makes and models and is administered by a third party, SD645 § 2—a system that does not exist today, *see, e.g.*, GM Tierney Decl. ¶ 9.

As NHTSA observed, this mandate would undermine existing safe and secure vehicle systems, which have been designed in accordance with NHTSA's "key recommendation" that "manufacturers should control access to firmware that executes vehicle functions," especially when that firmware "control[s] vehicle motion such as steering, acceleration, and braking." NHTSA Ltr. 3. Moreover, the Data Law's requirement of standardized access to on-board diagnostic systems would render inoperative an important design feature of the present "non-standardized approach": providing "cybersecurity benefits such that the scale and potential consequence of any specific cyberattack is inherently reduced." *Id.* at 4. As NHTSA explained, with a standardized approach, "a single successful malicious cyberattack could have a much wider scale of consequences because it can affect a larger number of vehicles." *Id.*

Second, the Data Law requires any manufacturer that "utilizes a telematics system" in its vehicles to develop and install in every vehicle sold in Massachusetts a standardized, open-access, bi-directional "platform." SD645 § 3. This platform must allow third parties unfettered access to use, modify, or write "any vehicle-specific data, including telematics system data, generated,

stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle" to the platform. *Id.* §§ 1, 3.

As NHTSA again explained, this requirement, too, would interfere with the operation of existing safe and secure vehicle systems, which—in accordance with NHTSA's "key recommendation"—employ "logical and physical isolation techniques" to "separate processors, vehicle networks, and external access points to limit and control pathways from external threat vectors to cyber-physical features of vehicles." NHTSA Ltr. 4. These layers of isolation are "important," NHTSA says, "because the best way to prevent a malicious hacker from remotely taking control of a vehicle or manipulating its performance is to ensure that there is no pathway by which external connections can access and send commands to in-vehicle components." *Id.* The Data Law requires manufacturers to render that important design feature inoperative, because it "specifically *require[s]* that vehicles be redesigned so that they are *not* isolated by mandating the ability to remotely 'send commands to in-vehicle components' such as steering, braking, and acceleration systems." NHTSA Ltr. 4 (quoting SD645 § 3).

Third, the Data Law imposes its novel requirements immediately. Section 2 of the Data Law goes into effect on December 18. SD645 § 2. And Section 3 of the Data Law goes into effect for model year 2022 vehicles, *id.* § 3—vehicles that have in large part already been designed, manufactured, and tested, and that members will be selling in the first quarter of the new year as soon as January 2021. GM Corsetti Decl. ¶ 3; *see also, e.g.*, FCA Decl. ¶ 5 (March 1, 2021); Honda Decl. ¶ 5 (Q1 2021); Decl. of Manish Mehrotra of Hyundai Motor North America ("Hyundai Mehrotra Decl.") ¶ 3 (March 2021); Mazda Decl. ¶¶ 5-6 (fall 2021); Subaru Lin Decl. ¶ 3 (spring 2021). There are no "existing system architectures that would satisfy the requirements of" the Data Law, nor could they realistically "be developed, tested, validated and deployed in the

proposed timeframe." NHTSA Ltr. 3; *see* FCA Decl. ¶¶ 6-28; Honda Decl. ¶¶ 8, 25; Mazda Decl. ¶¶ 8, 25; Subaru Lin Decl. ¶ 5; Subaru Yamamoto Decl. ¶ 8 Thus, the Data Law's requirements, coupled with its short timeframe for compliance, "would require [manufacturers] to remove all access controls from their telematics systems, including controls designed to ensure the security of safety-critical systems." Ltr. 3. The Data Law would, in NHTSA's words, "effectively prohibit wireless access controls in motor vehicles sold in the United States," raising "grave concerns" and "*substantial safety risks for American families.*" *Id.* (emphasis added).

The Data Law's requirement that Auto Innovators' members make inoperative existing access and security controls installed as part of the critical system components in their vehicle lineup conflicts with members' obligations under federal law.

Manufacturers install and maintain strict access controls on electronic vehicle systems in order to protect critical vehicle functions and, ultimately, the safety of the entire vehicle. FCA Decl. ¶¶ 17, 22-23; Ford Decl. ¶¶ 13, 15-16; GM Tierney Decl. ¶¶ 4-5, 7; Honda Decl. ¶¶ 18-19, 21; Mazda Decl. ¶¶ 19-22; Subaru Yamamoto Decl. ¶¶ 3-4, 6. That ensures that core vehicle functions such as steering, acceleration, braking, and the deployment of safety features like air bags are not compromised by cybersecurity risks. Those controls, therefore, are a key "part" of the "device or element of design" that allows vehicles to comply with federal motor vehicle safety standards. 49 U.S.C. § 30122(b).[6]

Under the Data Law, manufacturers must eliminate their ability to authorize access to on-board diagnostic systems and also open up all, or virtually all, vehicle systems for third parties to access, modify, or write new data to those systems at will. SD645 §§ 1-3. If manufacturers take

[6] Federal standards around core vehicle functions, after all, extend broadly to encompass "all vehicle" components involved in their safe operation *E.g.*, 49 C.F.R. § 571.124 (discussing the core vehicle function of acceleration).

those actions, they no longer will be able to ensure that those systems function safely because they would be open to inadvertent or intentional harm. FCA Decl. ¶¶ 12, 17-19, 27; Ford Decl. ¶¶ 19-20; Honda Decl. ¶ 26; Mazda Decl. ¶¶ 23-24, 26; Subaru Yamamoto Decl. ¶ 7.

Moreover, Auto Innovators' members—who have expended enormous resources to protect vehicles from potential cyber intrusions—are necessarily aware that removing access controls around their vehicle systems will render these important design elements inoperative. *See* FCA Decl. ¶¶ 9, 19, 27; Honda Decl. ¶ 26; Mazda Decl. ¶¶ 21, 23-24; Subaru Yamamoto Decl. ¶¶ 7, 9.[7] But the Vehicle Safety Act prohibits manufacturers from "knowingly mak[ing] inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard prescribed under this chapter." 49 U.S.C. § 30122(b).

No exception to Section 30122 would excuse members from knowingly making inoperative these critical access controls in an attempt to comply with the Data Law's requirements. The Vehicle Safety Act excepts from liability a manufacturer that "reasonably believes the vehicle or equipment will not be used (except for testing or a similar purpose during maintenance or repair) when the device or element is inoperative." 49 U.S.C. § 30122(b). But the Data Law does not limit the effects of its novel "open access" system only to periods when the vehicle is immobile. Once a third-party has read/write access to vehicle systems housing data

[7] It is indisputable that removing access controls governing vehicle systems will "make" those access controls "inoperative" within the meaning of the Vehicle Safety Act. As the law's legislative history confirms, there is no surer way to render something inoperative than to remove it or degrade its effectiveness. *See* Haake Decl. Ex. 10, H.R. Rep. No. 93-1452, 93 Cong., 2d Sess. (1974) ("Regarding the Secretary's authority to prescribe regulations defining the term 'render inoperative,' the conferees intend that these regulations should make it clear that the permanent removal, disconnection, or degradation of the safety performance of any such device or element of design is prohibited.").

"otherwise related to" diagnosis, maintenance, or repair, there is no way for a manufacturer to limit the impact of that read/write access only to times when the vehicle is immobile.

NHTSA recognized that the Data Law "effectively prohibit[s] wireless access controls in motor vehicles"—"including controls designed to ensure the security of safety-critical systems." NHTSA Ltr. 3. And NHTSA specifically raised an alarm about the Data Law's expected impact on "firmware controlling vehicle motion," *id.*—pointing specifically to controls over "braking, acceleration, and steering," *id.* at 2; *accord id.* at 3, 4.

Nor is there any realistic possibility of a federal regulatory exemption. To be sure, the Vehicle Safety Act empowers NHTSA to issue such exemptions. 49 U.S.C. § 30122(c)(1). But, to date, the agency has only done so to allow limited installations of on-off switches for air bags, and to exempt aftermarket vehicle or equipment modifications to enable people with disabilities to operate or ride as passengers in motor vehicles. 49 C.F.R. §§ 595.5, 595.6, 595.7. At no point has NHTSA suggested that it might consider exempting from the Vehicle Safety Act's make-inoperative provision the cybersecurity controls that limit access to and protect the safety of core vehicle functions; NHTSA has never provided a whole-cloth exemption for every vehicle make and model. NHTSA has done the opposite with respect to this very issue by continually calling attention to the need to maintain and strengthen, not eliminate or weaken, these important controls. *See, e.g.*, NHTSA Ltr; NHTSA, *Cybersecurity Best Practices for Modern Vehicles* (Oct. 2016).

To comply with the Data Law, Auto Innovators' members would therefore have to violate the Vehicle Safety Act—it would be "impossible" for them "to compl[y] with both state and federal law." *Oneok, Inc. v. Learjet, Inc.*, 575 U.S. 373, 377 (2015). If the Data Law is allowed to go into effect, manufacturers would yet again be put in a position where they cannot "comply with both state and federal requirements." *Myrick*, 514 U.S. at 287. The Data Law thus "stands

as an obstacle" (*Wood*, 865 F.2d at 408) to the federal requirements in the Vehicle Safety Act and is preempted.

B. The Data Law Is Preempted By The Clean Air Act.

The Data Law is also preempted by the Clean Air Act because Auto Innovators cannot "comply with both state and federal requirements" and the Data Law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress" in the Act. *Oneok*, 575 U.S. at 377. The Data Law would force members, in violation of federal law, "to remove or render inoperative" access controls members have in place to prevent tampering with vehicle emissions systems. 42 U.S.C. § 7522(a)(3)(A).

The Clean Air Act effectively nationalizes emissions-controls standards in new motor vehicles, preventing a patchwork of state regulation. Under the Act, no State "shall adopt or attempt to enforce any standard relating to the control of emissions" subject to the EPA's Clean Air Act authority. 42 U.S.C. § 7543(a). And the term "standard" relates broadly to the "emission characteristics of a vehicle or engine," including "not only 'numerical emission levels with which vehicles or engines must comply,' but also [the] 'emission-control technology with which they must be equipped." *In re Volkswagen "Clean Diesel" Mktg., Sales Practices, and Prods. Liab. Litig.*, 959 F.3d 1201, 1216-18 (9th Cir. 2020) (quoting *Engine Mfrs. Ass'n v. S. Coast Air Quality Mgmt. Dist.*, 541 U.S. 246, 252-53 (2004)).[8]

[8] The Clean Air Act imposes stringent vehicle-emissions requirements on manufacturers. For instance, it "requires manufacturers of new motor vehicles to warrant the emission control system of the vehicle for the 'useful life' of the vehicle"—either 10 years or 100,000 miles. *In re Volkswagen*, 959 F.3d at 1216 (citing 42 U.S.C. §§ 7521(d), 7541(a)(1)). It requires that manufacturers perform "in-use verification testing" on post-sale vehicles at regular mileage intervals prescribed by federal regulation. *See* 42 U.S.C. § 7541(a); 40 C.F.R. § 86.1845-04. And the EPA has the authority to require manufacturers to make changes to the configuration of vehicles, including changes to the vehicle's software to ensure that vehicles continue to meet federal emissions-control standards. *See* 40 C.F.R. § 86.1842-01(b). Failure to comply with the

The Clean Air Act's regulation of emissions controls is so comprehensive that the Act even preempts state regulations *designed to incentivize compliance with* federal standards pertaining to the emissions-control systems of new vehicles. For example, in *In re Volkswagen*, the challenged local regulations prohibited tampering with emissions-control systems in new vehicles in order to circumvent federal emissions standards. 959 F.3d at 1210-11. The court held that federal law preempted the regulations because they imposed a standard relating to the control of emissions and therefore were preempted by the Clean Air Act. *Id.* at 1217-18.

Here, the Data Law imposes a standard on Auto Innovators' members that will directly impact emissions-control technology in new vehicles. Indeed, the Data Law's standard *facilitates violations* of the Clean Air Act.

It is a violation of the Clean Air Act for any person "to install a defeat device on any motor vehicle at any time." *In re Volkswagen*, 959 F.3d at 1216-17 (citing 42 U.S.C. § 7522(a)(3)(B). A defeat device "reduces the effectiveness of an emission control system under conditions reasonably expected to be encountered in normal vehicle operation and use." *SEC v. Ustian*, 2019 WL 7486835, at *3 (N.D. Ill. Dec. 13, 2019). In recent years, the EPA has devoted significant agency resources to bringing over 50 cases against violators since 2015. *See* Haake Decl. Ex. 8, EPA News Release, *EPA Highlights Enforcement Actions Against Those Who Violate the Defeat Device and Tampering Prohibitions under the Clean Air Act* (Apr. 30, 2020), https://www.epa.gov/newsreleases/epa-highlights-enforcement-actions-against-those-who-violate-defeat-device-and. To date, EPA's efforts have resulted in multiple high-profile judgments against purveyors of

Clean Air Act and applicable EPA regulations can trigger significant penalties, including requirements to conduct a recall and remedy defects at the manufacturer's expense as well as civil enforcement actions. *See* 42 U.S.C. §§ 7524, 7541(c)(1), 7541(d).

defeat devices. *Id.* In some cases, these violators installed aftermarket defeat devices in tens of thousands of vehicles, demonstrating the considerable demand for these products. *Id.*

Emissions-control defeat devices often operate through the use of aftermarket software uploaded to vehicle systems. This "tuning software . . . hack[s] into and reprogram[s] a motor vehicle's electronic control module to alter engine performance and enable the removal of . . . critical emissions controls that reduce air pollution." Haake Decl. Ex. 6, EPA, News Release, *Punch It Performance and Tuning Agrees to Stop Selling Illegal Devices That Defeat Emissions Control Systems of Vehicles in the Wake of Clean Air Act Enforcement Action* (Jan. 10, 2020), https://www.epa.gov/newsreleases/punch-it-performance-and-tuning-agrees-stop-selling-illegal-devices-defeat-emissions. The use of such disabling software has the effect of dramatically increasing engine power at the cost of reducing or eliminating the effectiveness of required vehicle emissions controls. *E.g.*, FCA Decl. ¶ 27; Honda Decl. ¶ 23.

As discussed above, the Data Law requires manufacturers to eliminate their existing access controls and provide open access to their vehicle systems to read and modify vehicle data, as well as write new data to those systems. SD645 § 3. As a result of these required changes, vehicle owners (or third parties) would have ready access to a vehicle's engine control module to disable emissions control systems via software designed for that purpose. *E.g.*, FCA Decl. ¶¶ 7, 26-27; Honda Decl. ¶ 23 The Data Law thus hamstrings auto manufacturers from ensuring that their vehicles remain compliant with current emissions standards by facilitating violations of the Clean Air Act by third parties utilizing defeat devices to manipulate vehicle performance and circumvent emissions controls. FCA Decl. ¶¶ 6-9, 27; Honda Decl. ¶ 23; Toyota McFarland Decl. ¶ 6.

Manufacturers cannot enable the open access that the Data Law mandates without running afoul of the Clean Air Act. Section 203(a) of the Clean Air Act makes it unlawful "for any person

to remove or render inoperative any device or element of design installed on or in a motor vehicle or motor vehicle engine in compliance with regulations under this title prior to its sale and delivery to the ultimate purchaser." 42 U.S.C. § 7522(a)(3)(A). By requiring manufacturers to facilitate third-party access to critical vehicle systems affecting emissions (like the electronic control module), and foreclosing the ability of manufacturers to control that access, the Data Law invites the installation of defeat devices that the Clean Air Act prohibits. *Id.* § 7522(a)(3)(B). As a result, the Data Law is preempted by the anti-tampering provisions of the Clean Air Act. 42 U.S.C. § 7522(a)(3)(A), (B).

II. Auto Innovators' Members Are Likely To Suffer Irreparable Harm In The Absence Of Preliminary Relief.

To show irreparable harm, "a plaintiff need not demonstrate that the denial of injunctive relief will be fatal to its business." *Ross-Simons of Warwick, Inc. v. Baccarat, Inc.*, 102 F.3d 12, 18-19 (1st Cir. 1996). Rather, it need only show that it would "suffer[] a substantial injury that is not accurately measurable or adequately compensable by monetary damages." *Id.* Auto Innovators easily meets this burden. Absent a preliminary injunction, the Data Law would inflict several immediate and irreparable injuries that damages alone cannot remedy.

To begin with, Auto Innovators' members are in an impossible position because of the conflict between two irreconcilable regulatory regimes. For the reasons discussed above, members have existing statutory and regulatory duties under federal law that they will violate if they follow the Data Law's requirements—subjecting them to penalties under federal law. On the other hand, if they continue to follow federal law, they will be in violation of the Data Law. SD645 § 5. Compliance with one is mutually exclusive from compliance with the other.

Even more significantly, complying with the Data Law would compromise the integrity of members' vehicle systems. Members currently maintain a robust system of access and security

controls around their vehicle systems, which (as NHTSA recognizes) is critical to the safe operation of the vehicles they manufacture. FCA Decl. ¶¶ 22-23, 26; Ford Decl. ¶¶ 13, 15-16; Honda Decl. ¶¶ 18-19; Hyundai Robb Decl. ¶¶ 7-8; Mazda Decl. ¶¶ 17-20, 22; Subaru Yamamoto Decl. ¶¶ 3-4, 6 Among other things, the Data Law "would specifically *require* that vehicles be redesigned so that [vehicle systems] are *not* isolated" from each other, increasing the susceptibility to—and raising the scope and severity of—a cyberattack. NHTSA Ltr. 4.

Vehicle systems are already a prime target for cyberattack. *See, e.g.*, FCA Decl. ¶ 24; GM Tierney Decl. ¶ 6; Honda Decl. ¶ 20; Mazda Decl. ¶ 21; Subaru Yamamoto Decl. ¶ 5. A recent FBI report discussing cybersecurity risks in the auto industry noted that software developers were "able to commandeer the electric steering and brake control of a Jeep Cherokee . . . by wirelessly hacking into the car's main computer through an [on-board diagnostic II] connector." Haake Decl. Ex. 9, Chris Chin, *US Automakers Were Leading Targets for Hackers in 2018: FBI*, The Drive (Nov. 21, 2019), https://www.thedrive.com/tech/31150/fbi-claims-us-automakers-were-leading-targets-for-malicious-hackers-in-2018-report. By mandating *weaker* access controls, which take effect immediately, *see* SD645 §§ 2-3, the Data Law substantially increases the risk of system hacks with potentially disastrous consequences. That imminent risk of harm to the driving public is a classic "irreparable injury" because it "cannot adequately be compensated for either by a later-issued permanent injunction, after a full adjudication on the merits, or by a later-issued damages remedy." *Rio Grande Cmty. Health Ctr., Inc. v. Rullan*, 397 F.3d 56, 76 (1st Cir. 2005).

In addition to putting the public at risk, cybersecurity threats resulting from a lack of sufficient access controls will cause serious harm to a business's reputation. *Cf., e.g., Ross-Simons of Warwick, Inc. v. Baccarat, Inc.*, 217 F.3d 8, 13 (1st Cir. 2000) ("Because injuries to goodwill and reputation are not easily quantifiable, courts often find this type of harm irreparable."). Auto

Innovators' members have a strong interest in maintaining their reputation as manufacturers of secure and reliable vehicles. The Data Law threatens that reputation by requiring members to design and maintain telematics systems that third parties, without members' authorization, are able to access and modify at will. The increased risk of a serious cyberattack implicating customer safety that flows from the Data Law's "open access" systems risks permanently and immeasurably damaging members' reputations in the auto industry. *See, e.g.*, GM Copses Decl. ¶ 8; Subaru Lin Decl. ¶ 8. The Data Law leaves Auto Innovators' members in the position of running and being responsible for vehicle systems integral to safe and secure vehicle performance without having the ability to control access to those systems. SD645 §§ 2-3. That is a recipe for disaster. All it would take is one major hack with serious vehicle safety implications to injure the reputation for offering consumers safe and reliable vehicles that a manufacturer spent years building. *See, e.g.*, FCA Decl. ¶ 13; Subaru Lin Decl. ¶ 8. Yet, that is the inevitable consequence of the Data Law.

Members also run the risk of racking up substantial, unrecoverable costs once the Data Law takes effect, including the significant cost of recalls likely to be triggered by the law's vehicle safety implications. *See* FCA Decl. ¶ 13 (discussing how, after "cybersecurity researchers demonstrated vulnerabilities in certain FCA vehicles which allowed them wirelessly to take control of certain core vehicle functionalities . . . FCA recalled 1.4 million vehicles in coordination with NHTSA.") As a result of the short lead time between the Data Law's enactment and the effective date, Auto Innovators' members would have to incur significant financial costs right away in a (futile) attempt to satisfy the Data Law's requirements. *See, e.g.*, FCA Decl. ¶ 12-13; Subaru Lin Decl. ¶ 5; Toyota Stovall Decl. ¶ 16. Although such costs would ordinarily be recoverable from a private defendant, Auto Innovators' members are foreclosed from seeking damages from the Commonwealth. Courts routinely recognize that "where economic loss will be

unrecoverable, such as in a case against a Government defendant where sovereign immunity will bar recovery, economic loss can be irreparable." *Everglades Harvesting & Hauling, Inc. v. Scalia*, 427 F. Supp. 3d 101, 115 (D.D.C. 2019); *accord, e.g.*, *Kan. Health Care Ass'n v. Kan. Dep't of Soc. & Rehab. Servs.*, 31 F.3d 1536, 1543 (10th Cir. 1994) ("Because the Eleventh Amendment bars a legal remedy in damages, and . . . no adequate state administrative remedy existed . . . plaintiffs' injury was irreparable.").

Finally, there is no comprehensive way for Auto Innovators' members to mitigate the immediate impact of the Data Law. Members could, in theory, stop using altogether the telematics systems in the vehicles they sell in Massachusetts (to the substantial detriment of Massachusetts consumers). That could obviate having to comply with part of section 3 of the Data Law, which only applies to vehicles "that utilize[] a telematics system." SD645 § 3. But section 2 of the Data Law is not tied to whether telematics are enabled, nor are the Data Law's penalty provisions. *Id.* §§ 2, 5. And even section 3 of the law would still apply for members' vehicles sold in Massachusetts in aftermarket used sales. *Id.* § 3.

III. The Balance of Equities Weighs Heavily In Auto Innovators' Favor.

A preliminary injunction is warranted where, as here, the balance of equities favors the plaintiff. *E.g.*, *Ross-Simons of Warwick, Inc. v. Baccarat, Inc.*, 102 F.3d 12, 15 (1st Cir. 1996).

Auto Innovators' members will suffer immediate, significant hardship if the Data Law takes effect. Members will be forced to abandon the secure vehicle systems they have spent decades developing and instead (somehow) attempt to design, test, and deploy across their entire vehicle lineup "open access" systems that raise serious safety concerns within the span of a month, at most. SD645 §§ 2-3; *see also* FCA Decl. ¶¶ 12-13 GM Tierney Decl. ¶ 11; Mazda Decl. ¶ 26; Subaru Lin Decl. ¶ 5. The cybersecurity threats resulting from the Data Law would daily put at risk members' reputations in a competitive industry, with incalculable cost for any manufacturer

unlucky enough to be targeted by cyber attackers who can more easily exploit vehicle systems without a robust series of access controls. *See, e.g.*, *Zogenix, Inc. v. Patrick*, 2014 WL 1454696, at *2 (D. Mass. Apr. 15, 2014) (concluding that the balance of equities tipped in a drug company's favor due to its reputational injury from defendant's publicized ban of the drug, when that ban was likely preempted by the FDA's authority to issue the drug as safe for use).

The significant vehicle-safety, reputational, and economic injuries that Auto Innovators' members would suffer if subjected to the Data Law's directives far outweigh any costs from maintaining the status quo while the merits of the constitutionality of the Data Law are adjudicated. The public-facing purpose of the Data Law (according to its proponents) is to provide Massachusetts consumers with the ability to have their vehicles repaired at the independent repair shop of their choice. But they can do so now. Auto Innovators' members *already* provide access to any and all vehicle data necessary for diagnosis, repair, or maintenance. *E.g.*, BMW Decl. ¶ 10; FCA Decl. ¶ 14; Ford Decl. ¶¶ 15; GM Copses Decl. ¶ 5; Honda Decl. ¶ 10; Hyundai Rivera Decl. ¶ 2; Kia Thompson Decl. ¶ 4; JLR Decl. ¶ 8; Mazda Decl. ¶ 10; Subaru Decl. ¶ 7.

IV. An Injunction Is In The Public Interest.

It is axiomatic that "[p]rotecting public health and safety is in the public interest." *Zaya v. Adducci*, 2020 WL 2079121, at *8 (E.D. Mich. Apr. 30, 2020). Enjoining the Data Law thus will serve the public interest by ensuring that auto manufacturers do not have to abandon safe and secure vehicle systems for ones that NHTSA has recognized as posing substantial consumer safety risks. NHTSA Ltr. 3-4. When the federal regulator charged with auto safety has declared that public safety is at risk because of the Data Law, the public interest in preserving the status quo is unmistakable.

Enjoining the Data Law also will protect citizens of Massachusetts from the (perhaps unanticipated) environmental effects of the Data Law. Today's vehicles "emit far less pollution

than vehicles of the past," a feat "made possible by careful engine calibrations." Haake Decl. Ex. 7, EPA, *Punch It Performance Clean Air Act Settlement* (Jan. 10, 2020), https://www.epa.gov/enforcement/punch-it-performance-clean-air-act-settlement. But the installation of aftermarket defeat devices—something the Data Law will facilitate—threatens to "undo this progress, and pollute the air we breathe." *Id.* ("EPA testing has shown that a truck's emissions increase drastically (tens or hundreds of times, depending on the pollutant) when its emissions controls are removed.").

Moreover, as discussed above, the Data Law is unconstitutional under the Supremacy Clause because it is preempted by federal law. The public unquestionably has a strong interest in halting the enforcement of unconstitutional laws. *See, e.g.*, *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013) ("[The] enforcement of an unconstitutional law is always contrary to the public interest."); *United States v. Alabama*, 691 F.3d 1269, 1301 (11th Cir. 2012) ("[F]rustration of federal statutes and prerogatives are not in the public interest.").

CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court enter a preliminary injunction, in the form attached to Plaintiff's Motion as Exhibit A, barring the Data Law from taking effect.

Dated: December 1, 2020

Respectfully submitted,

ALLIANCE FOR AUTOMOTIVE INNOVATION

By its attorneys,

/s/ Laurence A. Schoen
Laurence A. Schoen, BBO # 633002
Elissa Flynn-Poppey, BBO# 647189
Andrew N. Nathanson, BBO#548684
MINTZ, LEVIN, COHN, FERRIS,
GLOVSKY, AND POPEO, P.C.
One Financial Center
Boston, MA 02111
Tel: (617) 542-6000
lschoen@mintz.com
eflynn-poppey@mintz.com
annathanson@mintz.com

Andrew J. Pincus (*pro hac vice*)
Erika Z. Jones (*pro hac vice*)
Archis A. Parasharami (*pro hac vice*)
Eric A. White (*pro hac vice*)
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
Tel: (202) 263-3000
apincus@mayerbrown.com
ejones@mayerbrown.com
aparasharami@mayerbrown.com
eawhite@mayerbrown.com

Charles H. Haake (*pro hac vice*)
Jessica L. Simmons (*pro hac vice*)
ALLIANCE FOR AUTOMOTIVE INNOVATION
1050 K Street, NW
Suite 650
Washington, DC 20001
Tel: (202) 326-5500
chaake@autosinnovate.org
jsimmons@autosinnovate.org

CERTIFICATE OF SERVICE

I hereby certify that the above and foregoing pleading was filed electronically through the Court's electronic filing system and that notice of this filing will be sent to all counsel of record in this matter by operation of the Court's ECF system and to non-registered users by first class mail.

Dated: December 1, 2020

/s/ Laurence A. Schoen
Laurence A. Schoen

105974160v1